International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.173-182
http://dx.doi.org/10.14257/ijsia.2016.10.3.16

Application of BP Neural Network Model based on Particle Swarm Optimization in Enterprise Network Information Security

Shumei liu

Hengshui University Center of Modern Educational Technology
Hengshui, Hebei 053000, China
lanxin0188@163.com

Abstract

The development of network technology has brought convenience to people's life, but also provides the convenience for the virus, Trojan and other destructive programs to attack the network. Then, the computer network security is becoming more and more dangerous. Accurately and scientifically predict the risk of network, it can effectively prevent the risk, and reduce the loss caused by the problem of computer network security. Computer network security is an early warning problem of multi index system. So, the traditional linear forecasting method cannot accurately describe the impact of each index on the evaluation results, and the accuracy of the prediction results is low. In order to improve the prediction accuracy of computer network security, this paper presents a new forecasting method for computer network security. Firstly, the evaluation index of computer network security is selected by expert system, and the weight of evaluation index is determined by the expert scoring method. Secondly, we put the index weight into the BP neural network, and use the BP neural network to learn it. Then, the parameters of BP neural network are optimized by the improved particle swarm optimization algorithm. After that, this paper uses a method based on the Fibonacci method principle to find the number of hidden layer node which has the best fitting ability. Finally, we use this algorithm to predict the network security of a certain enterprise in the next six months. The score is 0.67, 0.84, 0.72, 0.87, 0.86 and 0.91, which is close to the actual value of network security.

***Keywords**: particle swarm optimization, Fibonacci method, BP neural network, Network information security*

1. Introduction

Security early warning is a kind of active safety protection technology, which provides a useful complement to the protection mechanism of the firewall, such as providing a real-time protection against external attacks, internal attacks and misuse. Before the intrusion and attack to the system, the security early warning can detect intrusion and attack, and uses the alarm and control tools to operate the defense system. In the process of intrusion and attack, security warning can reduce the damage caused by intrusion and attack. After being attacked, the security warning system analyzes the intrusion information, and the intrusion information is added to the knowledge base as the information of system defense mode. So as to increase the defense capability of the system, and avoid being invaded in the same way. The development of network technology has brought convenience to people's life, but also provides the convenience for the virus, Trojan and other destructive programs to attack the network. The computer network security is becoming more and more dangerous. Accurately and scientifically predict the risk of network, it can effectively prevent the risk, and reduce the loss caused by the problem of computer network security. Therefore, strengthening the construction of enterprise network security

ISSN: 1738-9976 IJSIA

system and the research of security application mode has become the top priority of our country's enterprise informationization [1-4].

Foreign scholars have already carried out the research on the early warning system and intrusion detection technology, and have already carried out the monitoring of intrusion behavior in some important areas, such as military, political and economic networks. These systems play an important role in the discovery of intrusion attacks, analysis of intrusion detection technology and the protection of information network security[5-8]. Y Jim has designed a model which can predict the attack by constructing the attack profile, which includes the historical activity, the attack tools, the operation steps, the target, the motivation and so on. However, the network overhead of constructing attack profile is very large [9]. Ming Yuh Huang makes attack intention as an independent factor, and uses the target tree to model the attack intention, so as to predict the possible attack [10]. In our country, Miao Qing draws lessons from the research of foreign strategic warning system. He studies the attack detection technology and information fusion algorithm based on fuzzy neural network [11]. Liu Shaonan analyzes the different types of IDS, and proposes a network security early warning system based on network IDS and host IDS[12]. Hu Huaping proposes a network security early warning model, the model uses the regional threat degree, regional risk value and other threat evaluation factors to solve the problem of network threats [13]. Xu Yuantao designs a network security early warning system model, and the intrusion detection system provides data sources for his model[14]. Chen Yande designs and researches the network security situation awareness system. Network security situation is a new technology to achieve network security detection and warning [15].

Although some of the techniques in the early warning have been studied, and some achievements have been made, but there are few researches on the strategic early warning system. The study of the early warning system is still in the exploration stage. In order to improve the prediction accuracy of computer network security, this paper presents a new forecasting method for computer network security. Firstly, the evaluation index of computer network security is selected by expert system, and the weight of evaluation index is determined by the expert scoring method. Secondly, we put the index weight into the BP neural network, and use the BP neural network to learn it. Then, the parameters of BP neural network are optimized by the improved particle swarm optimization algorithm. After that, this paper uses a method based on the Fibonacci method principle to find the number of hidden layer node which has the best fitting ability.

2. Neural Network Mode

BP neural network is a multilayer feedforward neural network. It belongs to the error back propagation algorithm. It is composed of input layer, output layer and some hidden layer. Each layer has a plurality of nodes, each node represents a node of neuron with a connection between the upper and the lower nodes, and the nodes of the layer are connected with the layer by a full interconnection, and there is no association between each layer. As shown in figure 1.

The BP algorithm usually uses the sigmoid function as the excitation function. Next, we give several commonly used excitation functions.

(1) Threshold excitation function:

$$f(x)=\begin{cases}1, & x\geq 0\\ 0, & x\leq 0\end{cases}$$

(1)

(2) Sigmoid excitation function:

$$f(x)=\frac{1}{1+e^{-x}}$$

(2)

(3) Linear excitation function:

$$f(x)=kx$$

(3)

(4) Hyperbolic tangent excitation function:

$$f(x)=\tan(\frac{x}{T})$$

(4)

In this paper, we use the formula 2 as an excitation function of BP neural network. It satisfies the strict increasing property, it can make the output show a good balance in the linear and nonlinear. So, it can realize the input and output of any nonlinear mapping, and suitable for medium and long-term forecast. This function has the advantages of good approximation effect, fast calculation speed and high accuracy. At the same time, it's theory basis is perfect, the derivation process is rigorous, and the formula is symmetrical. It has strong nonlinear fitting ability, and it is suitable for small data processing.

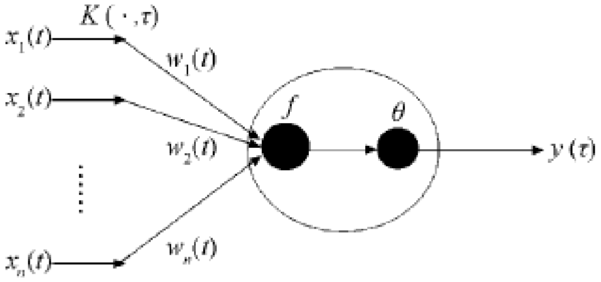

Figure 1. Topology of the BP Neural Network

3. Particle Swarm Optimization Algorithm

The particle swarm optimization algorithm is proposed by Kennedy and Eberhart. The algorithm is inspired by the foraging behavior of birds, and is used to solve the optimization problem. In the particle swarm optimization, the solution of each optimization problem is a bird in the search space, and the birds are called particles. Each particle has its own position, velocity, and the fitness value of a function that is determined by the optimized function. The particles follow the current optimal particles in the solution space. In each iteration, the particles update their positions by searching the two extreme values. The first one is the optimal solution, which is found by the particle itself. It is called the individual extreme value point, which is expressed by p_{best}. The other extreme value is the current optimal solution of the whole population. That is the global extreme value, which is expressed by g_{best}. There are m particles that form a group in a D-dimensional search space, and the particle swarm optimization algorithm can be described as follow:

The position of the i th particle is indicated by the $X_i=(x_{i1},x_{i2},\cdots,x_{id})$,（$i=1,2,\cdots,m$）, $V_i=(v_{i1},v_{i2},\cdots,v_{id})$ represents the speed of the i th particle, $p_{best}, i=(p_{i1},p_{i2},\cdots,p_{id})$ is the optimal location for the i th particle, and $g_{best}=(g_1,g_2,\cdots,g_d)$ is the optimal location for all particles in the group. To follow these two optimal values, the particle is updated by the formula (5) and (6) respectively, and the speed and position of the particles are updated to meet the conditions of the end of the iteration.

$$v_{id}^{k+1} = \omega^k v_{id}^k + c_1 r_1 (p_{id}^k - x_{id}^k) + c_2 r_2 (g_d^k - x_{id}^k)$$

(5)

$$x_{id}^{k+1} = x_{id}^k + v_{id}^k$$

(6)

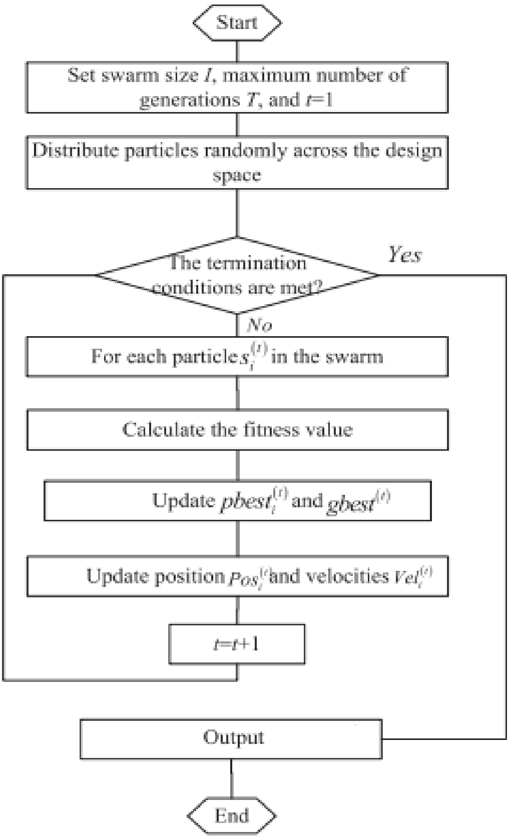
Start
Set swarm size I, maximum number of generations T, and t=1
Distribute particles randomly across the design space
The termination conditions are met?
Yes
No
For each particle $s_i^{(t)}$ in the swarm
Calculate the fitness value
Update $pbest_i^{(t)}$ and $gbest^{(t)}$
Update position $Pos_i^{(t)}$ and velocities $Vel_i^{(t)}$
t=t+1
Output
End

Figure 2. Algorithm Flow Chart

4. Improved Particle Swarm Neural Network Algorithm

Since the parameter of basic PSO is fixed, it is less accurate for some function optimization. In order to solve this problem, Eberhart and Shi introduced inertia weight to improve the algorithm. In each iteration, the velocity of particles is determined by the following formula:

$$v_i = \omega v_i + c_1 r_1 (p_i - s_i) + c_2 r_2 (g_d - s_i)$$

(7)

$$\omega = \omega_{\max} - (\omega_{\max} - \omega_{\min}) T_{\max} / T$$

(8)

Here, ω is the inertia weight. According to the number of iterations, the ω is dynamically adjusted. Thus, with the increase of the number of iterations, the ω is gradually reduced. The search area will be smaller and smaller, the convergence speed is faster, and the effect is better. In order to effectively control the particle velocity, and achieve the global and local effective balance, this paper constructs a PSO algorithm based on shrinkage factor, and its evolution equation is:

$$v_i = \theta[v_i + c_1 r_1 (p_i - s_i) + c_2 r_2 (g_d - s_i)]$$

(9)

$$\theta = \frac{2}{\left|2 - \varphi - \sqrt{\varphi^2 - 4\varphi}\right|}, \qquad \varphi = c_1 + c_2 \varphi \geq 4$$

(10)

In this model, θ is called a shrinkage factor, which is used to control the flight velocity of the particles. We combine the inertia weight ω and the convergence factor θ to get the improved speed equation. This improved PSO algorithm not only guarantees the convergence, but also accelerates the convergence rate and improves the accuracy of the solution.

$$v_i = \theta[\omega v_i + c_1 r_1 (p_i - s_i) + c_2 r_2 (g_d - s_i)]$$

(11)

Based on the characteristics of particle swarm optimization, the parameters of the neural network are integrated into the PSO model, and the overall optimization is carried out. This can make full use of the global search ability of particle swarm optimization, so that the algorithm of this paper can better play its powerful approximation ability.

5. Simulation Experiment and Result Analysis

5.1. Network Security Evaluation Index System

Network and information system is a complex system engineering, which includes the external factors and the internal factors, and they are mutually restricted. Therefore, we must have a standard, unified, objective criteria to measure network security. According to the domestic and foreign network security evaluation standard, and the basic requirements of the network and information system security, we should fully consider the various factors that affecting the security of the network, such as physical security factor, operation safety factor, information security factors, system security policy, safety technical measures, and safety management measures. Therefore, we give the network security evaluation index system. As shown in table 1:

Table 1. The Network Security Evaluation Index System

First level index	Second level index	safety index	Variable
network security	physical security	Equipment safety	X_1
		Environmental safety	X_2
		Media security	X_3
	operation safety	Risk analysis	X_4
		Access control measures	X_5
		Audit measures	X_6
		Emergency technology	X_7
	information security	Information transmission security	X_8
		Defense Technology	X_9
		Data integrity	X_{10}
		Data encryption	X_{11}
	system security policy	Database access control measures	X_{12}
		Database system state monitoring	X_{13}
		User identity authentication	X_{14}
		Data remote backup	X_{15}
		Security audit function	X_{16}

	safety technical measures	Anti-hacking measures	X_{17}
		Anti-virus measures	X_{18}
		System operation log	X_{19}
		Server backup	X_{20}
		Organization	X_{21}
	safety management measures	Regulations	X_{22}
		Accident emergency plan	X_{23}

5.2 Data Preprocessing of Network Security Index

Table 1 reflects the security of computer networks from different angles. As the dimensions of the various indicators are different, so we cannot make a direct comparison. In order to make the index have comparability, and to speed up the convergence rate of the neural network, this paper has carried on the normalized processing to each index:

1) For qualitative indicators: using expert scoring method to determine its data, and we have a normalized treatment of various indicators.

2) For quantitative indicators: the following formula is used to normalize.

$$x_i = \frac{x_i - x_{i\min}}{x_{i\max} - x_{\min}}$$

(11)

Where, the normalized values for the i th indicator is x_i, the minimum value of the i th indicator is $x_{i\min}$, and the maximum value of the i th indicator is $x_{i\max}$.

5.3 Simulation Experiment

In this paper, the computer network security data of an enterprise is selected, and all the indexes are scored by the experts. The result of the scoring is the input value of the improved BP neural network. Because the neural network model of this paper is a 23-X-1 model. We carry out the training of the sample according to principle. According to the Fibonacci method, the number of input layer node is k, the number of output layer node is l, and the number of hidden layer node is m.

Where the $m \in [a,b]$, and it satisfies the following formula:

$$a = (k+l)/2 \le m \le (k+l) + 10 = b$$

(12)

Step 1:

In this paper, $k = 23$ is the input layer node of BP neural network, and $l = 1$ is the output layer node. According to the formula 12, we can get $a = 12$ and $b = 34$. According to the Fibonacci method, we can get $g_1 = 18.796$ and $g_2 = 26.204$. g_1 is approximated by 19, and g_2 is approximated by 26. Then, we can get the values of fitting residual which is $E(g_1)$ and $E(g_2)$, as shown in Figure 3 and Figure 4.

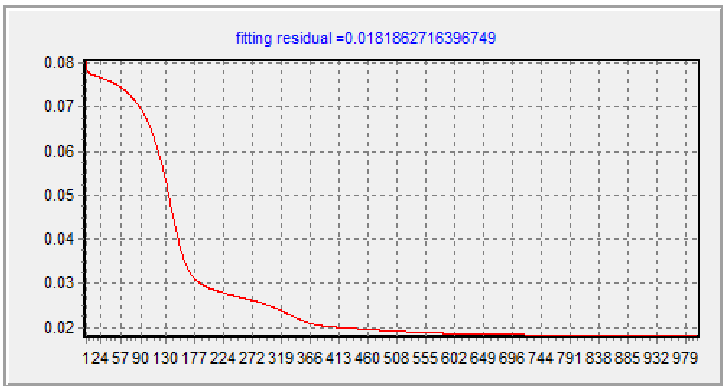

Figure 3. The Number of Hidden Layer Node is 19 in Neural Network Training

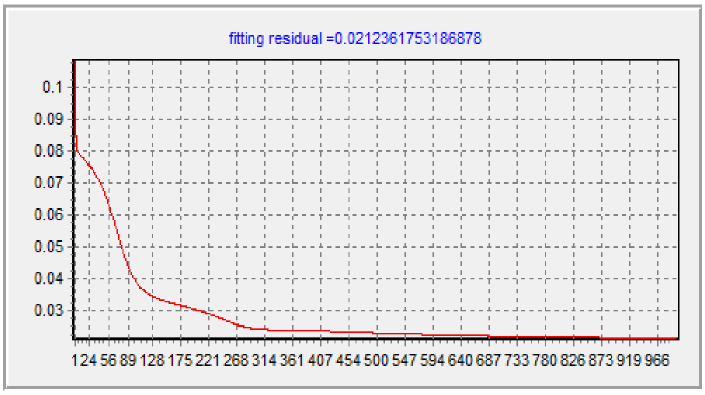

Figure 4. The Number of Hidden Layer Node is 26 in Neural Network Training

We can see from the figure of training results, the number of hidden layer node is 19 that the fitting residual is 0.0181, and the number of hidden layer node is 26 that the fitting residual is 0.0212. That is to say the $E(g_1) < E(g_2)$. According to the principle of the Fibonacci method, we keep the $[12, 26]$, and give up $(26, 34]$.

Step 2:

According to the Fibonacci method, we can get $g_3 = 18.023$ and $g_4 = 20.105$. g_3 is approximated by 18, and g_4 is approximated by 20. Then, we can get the values of fitting residual which is $E(g_3)$ and $E(g_4)$, as shown in Figure 5 and Figure 6.

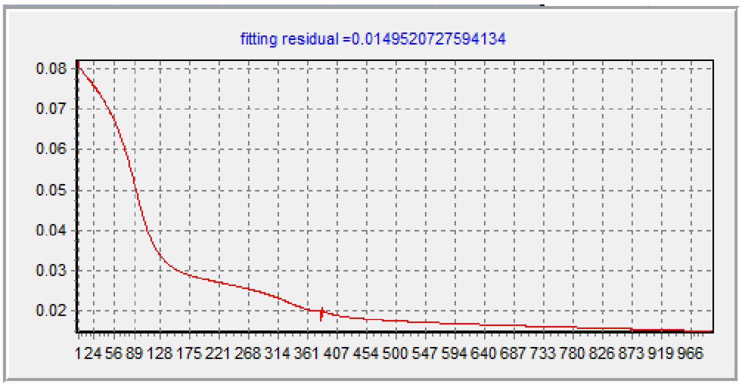

Figure 5. The Number of Hidden Layer Node is 18 in Neural Network Training

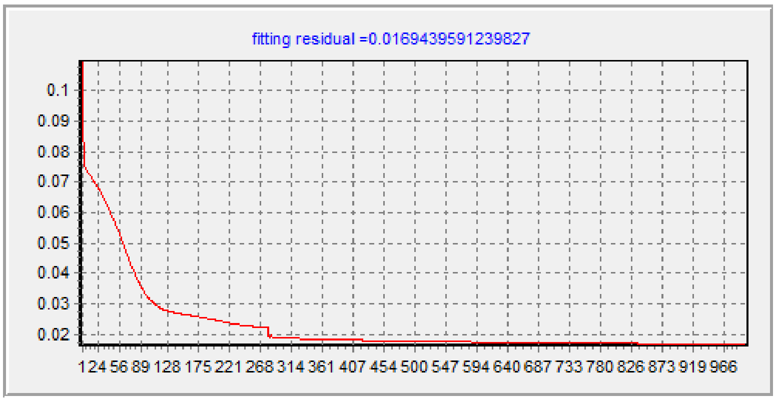

Figure 6. The Number of Hidden Layer Node is 20 in Neural Network Training

We can see from the figure of training results, the number of hidden nodes is 18 that the fitting residual is 0.0149, and the number of hidden layer node is 20 that the fitting residual is 0.0169. That is to say the $E(g_3) < E(g_4)$ .According to the principle of the Fibonacci method, we keep the $[12, 20]$, and give up $(20, 26]$.

Step 3:

According to the Fibonacci method, we can get $g_5 = 14.153$ and $g_6 = 17.795$. g_5 is approximated by 14, and g_6 is approximated by 18. Then, we can get the values of fitting residual which is $E(g_5)$ and $E(g_6)$, as shown in Figure 7 and Figure 5.

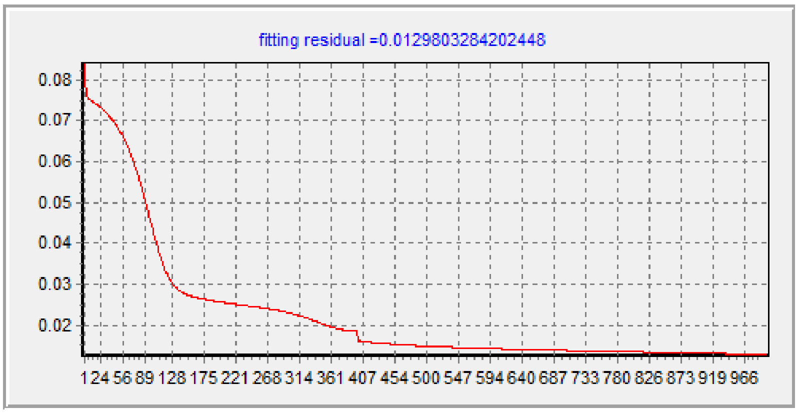

Figure 7. The Number of Hidden Layer Node is 14 in Neural Network Training

We can see from the figure of training results, the number of hidden nodes is 14 that the fitting residual is 0.0129, and the number of hidden layer node is 18 that the fitting residual is 0.0149. That is to say the $E(g_5) < E(g_6)$ .According to the principle of the Fibonacci method, we keep the $[12,18]$, and give up $(18, 20]$.

Step 4:

According to the Fibonacci method, we can get $g_7 = 14.854$ and $g_8 = 15.031$. g_7 and g_8 is approximated by 15. Finally, we keep the number of hidden layer node is 15. As shown in Fig 8.

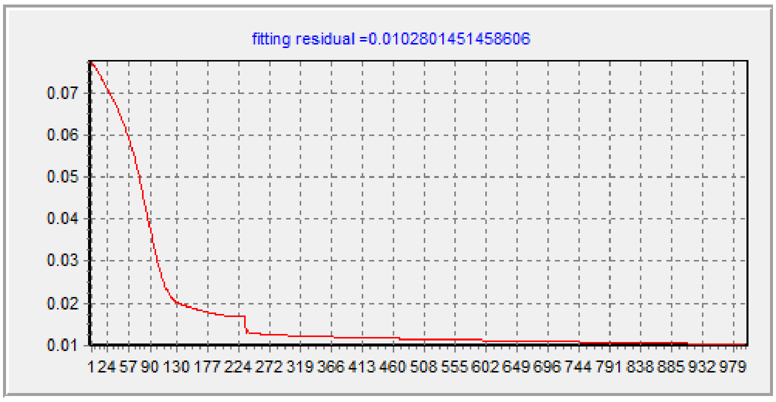

Figure 8. The Number of Hidden Layer Node is 15 in Neural Network Training

Above all, when number of hidden layer node of the BP network is 15, the mean square error reaches the minimum, which is 0.0102. Thus, an improved BP neural network model trained with 15 hidden layer nodes is completed.

5.4 Setting of Computer Network Security Level

According to the comprehensive score of the index, we can evaluate the computer network security. According to the relevant research, the computer network security level is divided into 4 levels. They include that safety (A), basic safety (B), insecurity (C) and extreme insecurity (D). We set the total score of security level to 1, then the corresponding security level and the corresponding score is shown in table 2.

Table 2. Computer Network Security Level

level	A	B	C	D
Score	1-0.85	0.85-0.7	0.7-0.6	0.6-0

Next, we select a company's computer network security data as sample data. Then, all the indicators of 48 months has to be marked by the experts. We put the results of the score as the input value of the improved BP neural network model. Through this paper's excitation function, we can output the computer network security score of the enterprise in the next six months. According to figure 8, we can know that the improved BP neural network model is a 23-15-1 model. Then, we use this algorithm to compare with other methods which are artificial neural network prediction algorithm and gray forecasting model. Experimental results show that the prediction results are more close to the expected output value of the enterprise.

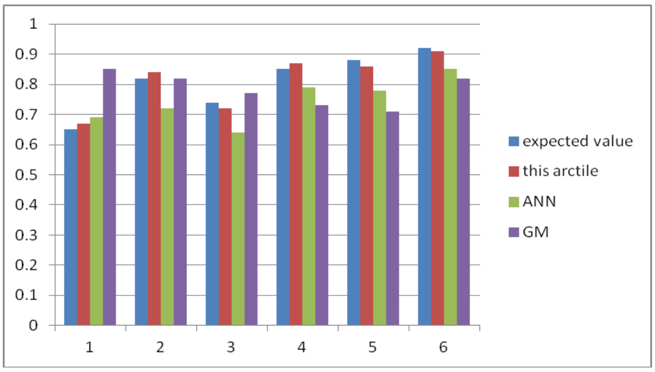

Figure 9. Comparison Chart of the Forecasting Result

6. Conclusion

In order to improve the prediction accuracy of computer network security, this paper presents a new forecasting method for computer network security. Firstly, the evaluation index of computer network security is selected by expert system, and the weight of evaluation index is determined by the expert scoring method. Secondly, we put the index weight into the BP neural network, and use the BP neural network to learn it. Then, the parameters of BP neural network are optimized by the improved particle swarm optimization algorithm. After that, this paper uses a method based on the Fibonacci method principle to find the number of hidden layer node which has the best fitting ability. Finally, we use this algorithm to predict the network security of a certain enterprise in the next six months. The score is 0.67, 0.84, 0.72, 0.87, 0.86 and 0.91, which is close to the actual value of network security.

Reference

[1] China Internet Network Information Center, Statistical report on Internet development in China, **(2013)**.

[2] National Internet Emergency Center, China Internet Network Security Report, http://www.cert.org.cn/publish/main/46/2012/20120523085533341215471/20120523085533341215471_.html, **(2011)**.

[3] Institute C S. 2010/2011 CSI Computer Crime and Security Survey, http://gocsi.com/survey.

[4] China Internet Network Information Center, Statistical report on Internet development in China, **(2012)**.

[5] A. Rathmell, R. Overill and L. Valeri, "Information Warfare Attack Assessment System[EB/OL]", http:www.kcl.ac.uk/orgs/icsa/old/iwaasppr.pdf, **(1997)**.

[6] ADCT.FY Information Assurance: Automated Intrusion Detection Environment[EB/OL], http://www.acq.osd.mil/actd/descript.html, **(1998)**.

[7] A. Rathmell, J. Dorsehner and M. Knights, "Summary of Research Results: Threat Assessment and Early Warning Methodologies for Information Assurance [EB/OL]", http.iaac.org.uk/Publications/ROPA/Website%20summary.pdf, **(2003)**.

[8] "The national strategy to secure cyberspace [EB/OL]", http://www.us-cert.gov/reading room/caberspace_strategy.pdf, **(2003)**.

[9] J. Y. Shyhtsun, W. Felix, G. Fengmin and M. Yuh, "Intrusion Detection for an On-GoingAttack[EB/OL]", http://www.mnlab.cs.depaul.edu/seminar/fall2002/IDSonGoing.pdf, **(l999)**.

[10] H. Ming-Yuh, R. J. Jasperand T. M. Wicks, "A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis", Computer Networks, vol. 31, **(1999)**, pp. 2465-2475.

[11] M. Qing, "Research on the design and key technology of network security strategy early warning system", Hunan: National Defense Science and Technology University, **(2002)**.

[12] S. Liu, X. Li and P. Wang, "Design of network security early warning system", Computer science, vol. 31, no. 10, **(2004)**, pp. 276-277.

[13] H. Hu, L. He, F. Xiao and Q. Zhang, "Research on network security early warning model", Computer research and development, vol. 43, **(2006)**, pp. 353-359.

[14] Y. Xu, J. Zhang, J. Huang and B. Wang, "Preliminary study on network security early warning system", Computers and telecommunications, vol. 7, **(2007)**, pp. 27-30.

[15] Y. Chen, L. Zhao, Q. Wang, Z. Pan and Z. Zhou, "Research on the structure of network security situation awareness system", Computer engineering and applications, vol. 44, no. 1, **(2008)**, pp. 100-102.